[인용발명2 1부]

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[6]
G06F 15/00

(11) 공개번호 특1998-042805
(43) 공개일자 1998년08월17일

(21) 출원번호 특1997-063284
(22) 출원일자 1997년11월27일
(30) 우선권주장 8/780,817 1997년01월09일 미국(US)
(71) 출원인 선마이크로시스템스,인코퍼레이티드
미국, 캘리포니아 94303, 팔로 알토, 산 안토니오 로드 901
(72) 발명자 레노드반자민제이.
미국, 캘리포니아 94062, 우드사이드, 챔프먼 로드 152
팸퍼혁존씨.
미국, 캘리포니아 95037, 모간 힐, 바리트 애비뉴 735
호지스월셔애브릴이.
미국, 캘리포니아 94301, 팔로 알토, 이머슨 스트리트 1085
(74) 대리인 강명구

심사청구 : 있음

(54) 자료파일내 자료가 진짜임을 검증하기 위한 방법, 장치 및 프로덕트

요약

본 발명은 하나 또는 둥이상의 자료파일내 자료의 진짜임을 검증하기 위한 방법, 장치 및 프로덕트를 제공하는 것이다. 본 발명의 한 특징에 따라, 자료의 진짜임을 검증시키기 위한 방법이 한 식별기를 포함하는 적어도 하나의 자료파일 그리고 디지탈 기호뿐 아니라 자료파일에 대한 식별기를 포함하는 기호파일을 포함한다. 다음에 디지탈 기호가 컴퓨터 시스템을 사용하여 검증되며, 다음에 자료파일내 식별기가 컴퓨터 시스템을 사용하여 기초파일내 식별기와 비교된다.

한 실시예에서, 자료파일 식별자는 적어도 하나의 증명서 권한, 사이트 증명서, 소프트웨어 공표자 식별자 또는 사이트 이름을 포함하며, 자료의 진짜임을 검증하는 것이 증명서 권한, 사이트 증명서, 소프트웨어 공표자 식별자 그리고 상기 사이트 이름중 적어도 하나에 대한 보안 수준을 정함을 포함한다.

대표도

도2

명세서

도면의 간단한 설명

도 1 은 네트워크된 계산 환경을 도시한 도면.

도 2 는 도 1 의 네트워크된 계산 환경과 함께 사용하기 위한 대표적인 컴퓨터 시스템을 도시한 도면.

도 3a 는 본 발명의 실시예와 함께 사용하기 위한 기초파일을 포함하는 기록 보관 자료 구조의 실시예를 도시한 도면.

도 3b 는 본 발명의 실시예와 함께 사용하기 위한 기초 파일을 한 실시예를 도시한 도면.

도 4 는 기호파일을 갖는 자료 구조와 함께 사용하기 위한 본 발명 실시예의 흐름도.

도 5 는 본 발명의 실시예에 따라 보안 관리자내 보안 수준을 정함과 관련된 단계를 설명하는 흐름도.

도 5a 는 본 발명의 실시예에 따라 개선된 세팅을 설명하는 브라우저(browser) 인터페이서를 대략적으로 도시한 도면.

제 6 은 본 발명의 실시예에 따라 검증 세팅을 사용하는 애플릿을 실행함과 관련된 단계를 설명하는 흐름도.

도 7 은 본 발명의 실시예에 따라 컴퓨터 네트워크 연결을 만드는 것과 관련된 단계를 설명하는 흐름도.

* 부호설명

10 ... 네트워크 계산 환경 12 ... 소스 사용자 컴퓨터
14 ... 수신자 사용자 컴퓨터 16 ... 자료 링크

20 ... 컴퓨터 시스템 22 ... 처리기
24 ... 주 메모리 26 ... 보조(이차) 메모리
28 ... 입출력 장치 30 ... 네트워크 통신 인터페이스
32 ... 버스

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 계산 자원 가운데 자료의 공유에 대한 것이다. 특히, 본 발명은 계산 시스템을 통하여 처리되는 자료가 진짜임을 확인하고 입증하기 위한 방법, 장치 및 프로덕트에 대한 것이다.

인터넷과 같은 네트워크 계산 환경이 더욱 보편화됨에 따라, 네트워크로 연결된 컴퓨터 가운데 공유된 정보를 안전하게 전송시키기 위한 필요가 그만큼 중요하게 되었다. 가령, 인터넷의 사용자가 자료 형태의 정보를 또다른 사용자에게 전송하는때 수신자가 수신된 자료가 변조되거나 어떤형태로 변경되지 않았음을 입증할 수 있다면 유용할 것이다. 또한, 수신자는 수신된 자료가 가짜가 아닌 올바른 송신자에 의해 송신되었음을 입증한다면 유익할 것이다.

결과적으로, 컴퓨터 네트워크 및 다른 자료 링크를 통해 전송되는 자료의 보안은 어느정도 개선되었다. 더욱더 안전한 방법은 모든 또는 일부의 자료를 그것을 전송하기전에 암호화하고, 수신된 자료를 마찬가지로 사용하기전에 해독함을 포함하는 것이다. 이같은 암호화와 해독기술은 암호화 자료를 자료 파일로 추가하고 암호화하며 혹은 기호 알고리즘을 실행하므로써 자료 파일내 자료를 컴퓨터 시스템으로 변환시킴을 포함한다.

오늘날 사용되고 있는 여러개의 기호 알고리즘이 있다. 한가지 널리 알려진 기호 알고리즘은 메시지 다이제스트 알고리즘과 RSA 암호화 알고리즘(가령 RSA를 갖는 MD5, 또는 RSA를 갖는 MD2 등)의 조합이다. RSA 기호 알고리즘을 갖는 메시지 다이제스트는 Redwood City 의 RSA Data Security, Inc. 로 부터 구입될 수 있다. 또다른 널리 알려진 기호 알고리즘은 DSA 암호화 알고리즘이다. 내국정부로 부터 입수될 수 있는 DSA 암호화 알고리즘은 기호 알고리즘으로서 개인들이 제한된 목적으로 사용될 수 있다. 이들 기호 알고리즘은 하기에서 상세히 설명된다.

RSA 알고리즘을 갖는 메시지 다이제스트로는 자료 파일로 추가될 수 있는 디지탈 기호(signiture)를 발생시키는 능력이 있다. 디지탈 기호는 기본적으로 이를 통해 수신된 자료 파일 소스의 진짜 여부를 밝힐 수 있는 메카니즘이다. 디지탈 기호는 기본적으로 다른 사용자에게 관련된 자료파일과 함께 발생되고 제공될 수 있는 특수한 자료순서이다. 대부분의 신호 알고리즘뒤의 기본 개념은 모든 사용자(가령, 개인, 회사, 정부등)가 사설 키이(private key)와 공공 키이(pulic key) 모두를 포함하는 키이 쌍을 갖는다는 것이다.

가령, 키이는 변호 순서일 수 있다. 사설 키이는 한 사용자에게 할당되고 동 사용자에 의해 비밀로 유지되도록된 독특한 키이다. 상기 사설 키이는 기호 알고리즘으로 자료 파일에 대한 디지탈 기호를 발생시키도록 할당된 사용자에 의해 사용될 수 있다. 한편 공공키이는 모든 다른 사용자가 이용할 수 있도록 만들어진다. 공공키이는 이를 다른 사용자에 의해 사용되어 수신된 자료 파일에서의 디지탈 기호가 진짜임을(즉, 디지탈 기호가 사설 키이로 발생됨을)입증하도록 한다. 입증처리는 같은 기호 알고리즘으로 달성된다. 기본적으로, 이같은 입증처리는 수신된 자료 소스의 진위에 대한 자신감에 비교적 높은 수준을 제공한다.

알고리즘을 발생시키는 디지탈 기호에 추가하여, 자료파일이 어떤 방법으로 오염되어졌는가를 밝히도록 사용될 수 있다. 이들 알고리즘은 단일 방향 해쉬(hash) 기능으로 알려져 있다. 이같은 단일 방향 해쉬 기능은 대개 키이를 필요로 하지 않는다. 단일 방향 해쉬 기능은 자료 파일내로 삽입되는 추가의 자료를 포함한다. 마찬가지로, 자료파일이 수신되고 해쉬 기능이 해쉬 기능의 발생이후 자료 파일내의 자료 어느것도 변경되지 않았음을 입증하도록 사용될 수 있다. 그러나, 해쉬 기능은 가령 누가 그것을 보냈는지와 같은 관련 파일에 대한 어느것도 추측할 필요가 없다는데서 제한된다. 많은 기호 알고리즘은 내부의 빌딩블록과 같은 한 방향 해쉬기능을 사용한다.

인터넷과 같이 비교적 개방되고 보안이 되지않는 네트워크에서, 수신된 자료 파일을 의도된대로 사용하기전에 사용자가 수신된 자료파일의 진짜임을 파악하기 위해 사용될 수 있다. 이같은 자료파일은 컴퓨터 프로그램, 그래픽, 텍스트, 사진, 오디오, 비디오 또는 컴퓨터 시스템내에서 사용하기에 적합한 다른 정보를 포함한다. 자료파일의 타입과는 관계없이, 진짜임을 파악하는 것은 상기에서 설명된 바와같이 기호 알고리즘 또는 유사한 타입의 암호화 알고리즘으로 달성될 수 있다. 가령, 자료 파일이 소프트웨어 프로그램이면, 사용자는 프로그램이 바이러스로 사용자의 컴퓨터를 감염시키는 Trojan Horse를 포함하지 않도록 자신의 컴퓨터 시스템이 소프트웨어 프로그램에 노출되기전에 믿을 수 있는 자에 의해 전송된 것인가를 파악하기를 희망할 것이다. 이와같은 경우, 전송 사용자는 상기에서 설명한 바와같이 자료가 진짜임을 파악할 수 있다.

또다른 예는 자신의 컴퓨터 스크린상에 이를 표시하기전에 텍스트 또는 영상 자료파일이 파악하고자 하는 경우이다. 이는 바람직하지 않은 내용을 갖는 텍스트 및 영상의 표시장치를 제어하도록 사용될 수 있다. 가령, 부모들은 자녀들이 성인대상의 그림이나 텍스트에 접근하는 것을 제한하고자 할 것이다. 이는 그같은 자료파일(가령, 텍스트 또는 영상파일)이 믿을 수 있는 소스로 부터 오는가를 입증하므로써 달성될 수 있다. 이와유사하게, 텍스트 또는 영상파일의 제공자는 승인의 스탬프(도장)을 제공하여 거래이를 및 다른 지적재산의 사용을 제어하도록 할 수 있다.

불행하게도, 그와같은 암호화와 해독, 사인(sign)과 확인, 그리고 해쉬기능의 발생은 사용자의 계산 자원을 전송하고 수신하는데 대한 추가의 부담을 주게된다. 이같은 추가의 부담은 여러개의 자료 파일들을 전송 및 수신하는 사용자에게는 심각한 것이다. 일례로서, World-Wide Web 로 알려진 인터넷에서 그같은 부담이 커지므로써 사용자 사이 멀티플 자료 전송에서 엄청난 증가를 가져왔다. 이들 멀티플 자료파일들은 자바(Java™) 애플릿(applet)과 같은 목적-오리엔트 소프트웨어 쳐리를 구성하는 컴포넌트 또는 목적을 포함한다. 멀티플 자료파일 전송시 수신 사용자의 컴퓨터 자원에 가해질 수 있는 잠정적인 이같은 부담을 설명하기 위해, 파일 각각에 대한 디지탈 기호를 입증함과 관련된 결과의 처리시간을 계산하기만 하면된다. 가령, 자바™ 애플릿은 200개의 디지탈식으로 사인된 자바™ 클레스 파일(자료파일 포함)을 포함하면, 평균 확인 처리에 종래의 데스크탑 PC에서 약 1 초가 걸릴 것으로 가정할 때 사용자는 애플리을 사용하기 위해 자료 파일을 수신한 뒤에 약 200초를 기다려야 할 것이다. 이같은 지연은 이같은 컴퓨터 네트워크 환경의 효과를 크게 줄인다. 이는 스트림잉 오디오 또는 실시간(또는 실시간에 가까운)에 가까운 비디오 자료 파일과 같은 때에 알맞은 처리와 관련된 자료파일에 있어서 특히 정확하게 적용된다.

따라서, 필요한 것은 특히 컴퓨터 네트워크를 통해 전달되어질 자료파일의 경우 자료파일의 진짜임을 검증하기 위한 더욱더 효율적인 방법, 장치 및 프로덕트를 제공하는 것이다.

본명이 이루고자하는 기술적 과제

본 발명은 컴퓨터 네트워크를 통해 전달되어질 자료파일과 같은, 자료파일의 진짜임을 검증하기 위한 더욱더 효율적인 방법, 장치 및 프로덕트를 제공하는 것이다. 본 발명의 한 특징에 따라, 자료의 진짜임을 검증시키기 위한 방법이 한 식별자를 포함하는 적어도 하나의 자료파일 그리고 디지탈 기호를 마니라 자료파일에 대한 식별기를 포함하는 기호파일을 포함한다. 다음에 디지탈 기호가 컴퓨터 시스템을 사용하여 검증되며, 다음에 자료파일내 식별기가 컴퓨터 시스템을 사용하여 기호 파일내 식별기와 비교된다.

한 실시예에서, 자료파일 식별자는 적어도 하나의 증명서 권한, 사이트 증명서, 소프트웨어 공표자 식별자 또는 사이트 이름을 포함하며, 자료의 진짜임을 검증하는 것이 증명서 권한, 사이트 증명서, 소프트웨어 공표자 식별자 그리고 상기 사이트 이름중 적어도 하나에 대한 보안 수준을 정함을 포함한다. 이와같은 한 실시예에서, 자료파일은 컴퓨터 시스템을 다운로드(적재)되며, 만약 자료파일 애플릿이고 디지탈 기호가 검증되면, 다음에 자료의 진짜임을 입증하는 것이 애플릿을 이에 따라 브랜딩하고 실행함을 포함한다.

본 발명의 또다른 특징에 따라, 식별자를 포함하는 적어도 하나의 자료파일, 그리고 한 디지탈 기호에 추가하여 자료파일에 대한 식별기를 포함하는 기호파일의 진짜임을 검증하기 위한 장치가 디지탈 기호를 검증하기 위한 검증기 그리고 자료파일내 식별기를 기호파일내 식별기와 비교하기 위한 비교기를 포함한다. 한 실시예에서, 디지탈 기호는 한 기호 알고리즘으로 검증된다. 또다른 실시예에서, 비교기는 한 방향 해쉬 기능 알고리즘을 포함한다.

본 발명의 또다른 특징에 따라, 식별기를 포함하며 자료파일에 대한 식별기를 가지는 기호파일과 관련된 자료파일의 진짜임을 검증하도록 배열된 컴퓨터 시스템이 쳐리기, 이 쳐리기에 결합된 메모리, 그리고 디지탈 기호를 검증하고, 자료파일내 검증기를 기호파일내 검증기와 비교하기 위한 검증기를 포함한다. 한 실시예에서, 자료파일의 검증기는 적어도 하나의 증명서 권한, 사이트 증명서, 소프트웨어 식별자, 그리고 사이트 이름중 적어도 하나를 포함한다. 이같은 실시예에서, 검증기는 증명서 권한, 사이트 증명서, 소프트웨어 공표기 식별자, 그리고 사이트 이름중 적어도 하나의 보안 수준을 정하도록 된다. 또다른 실시예에서, 자료파일은 애플릿되며, 검증기는 애플릿을 브랜드하고 이 애플릿을 실행하도록 된다.

하기에서는 첨부도면을 참조하여 본 발명을 상세히 설명한다.

본명의 구성 및 작용

본 발명의 여러 실시예는 임의 수의 자료파일에 대한 단일 디지탈 기호만의 검증을 필요하므로써 사용자 컴퓨터 시스템을 발생시키는 곳과 수신하는 곳 모두에서의 계산 명령을 줄이는 신규한 방법, 장치 및 프로덕트를 제공한다. 본 발명의 실시예에 따라 자료파일은 개별적으로 사인될 필요가 없다. 대신에, 분리된 기호파일이 발생되어 분리된 기호파일이 디지탈식으로 표시되고 나중에 검증되는때 해당하는 자료파일이 이들 자료파일들 각각에 대한 기호 알고리즘을 실행하지 않고 확증될 수 있도록 한다. 한 실시예에서는 기호파일이 전달되어질 자료파일 각각과 관련된 한 방향 해쉬 기능과 같은 식별기 목록을 포함한다. 기호파일은 자료파일 각각에 대한 디지탈 기호와 동등한 암호이다.

따라서, 본 발명의 실시예로, 사용자는 각 자료파일에 대한 식별자들을 포함하는 신호파일을 발생시킬 수 있다. 사인된 신호파일과 자료파일은 수신하는 사용자에게 보내질 수 있으며, 사용자 적절한 신호 알고리즘을 사용하여 디지탈 기호를 검증할 수 있다. 일단 디지탈 기호가 검증되면, 기호파일내의 식별자는 자료파일내의 식별자와 비교될 수 있다. 주어진 자료파일내의 식별자가 기호파일내의 해당 식별자와 부합하면, 다음에 자료파일이 진짜인 것으로 검증된다.

다음에 수신 사용자가 진짜임에 자신감을 갖는 검증된 자료파일을 처리하도록 진행할 수 있다. 결과적으로, 더이상 디지탈 식으로 기호를 표시할 필요가 없으며 나중에 자료파일 각각에 대한 디지탈 기호를 검증할 필요가 없기 때문에 계산지연이 줄어들 수 있다.

도 1 은 수신기 사용자 컴퓨터 시스템(14)과 자료링크(16)를 통해 자료형태의 정보를 교환하기 위해 결합된 소스 사용자 컴퓨터 시스템(14)의 블록도표에 의해 네트워크 계산환경(10)을 설명하는 도면이다. 소스 사용자 컴퓨터 시스템(12)은 인터넷과 연결된 웹브 서버와 같은 서버 컴퓨터 형태를 한다. 마찬가지로, 수신기 사용자 컴퓨터 시스템(14)은 자료링크(16)를 통해 웹브 서버에 연결된 클라이언트 시스템 형태를 한다. 따라서 이와같은 경우에, 자료링크(16)는 인터넷 및 다른 연결된 네트워크의 일부나 전부를 나타낸다. 자료링크(16)는 하나나 둘 이상의 지역 네트워크(LANs), 광역 네트워크(WANs), 인트라네트 또는 엑스트라네트 혹은 통신 자료 네트워크 등을 나타낸다.

도 2 는 도 1 에 따라 송신 사용자 또는 수신 사용자 누구에 의해서도 사용될 수 있는 대표적인 컴퓨터 시스템(20)을 도시한 것이다. 선택에 따라, 컴퓨터 시스템(20)은 컴퓨터 사용가능 프로덕트를 통해서 자료를 수신할 수 있는 스탠드형(Stand-alone) 컴퓨터일 수 있다. 컴퓨터 시스템(20)은 하나나 둘이상의 처리기(22), 주메모리(24), 보조 또는 이차 메모리(26), 하나나 둘이상의 입력/출력(I/O) 장치(28), 하나나 둘이상의 네트워크 통신장치(30), 그리고 하나나 둘이상의 버스(32)를 포함한다.

처리기(22)는 컴퓨터 지시를 실행하기 위한 능력을 제공한다. 가령, 처리기(22)는 통상적으로 구입될 수 있는 데스크탑, 랩탑, 워크스테이션, 그리고 메인프레임 컴퓨터와 같은 마이크로처리기, 중앙처리장치(CPUs), 혹은 마이크로 제어기일 수 있다. 처리기(22)는 또한 특수한 목적 또는 더욱 큰 프레임 컴퓨터, 통신 스위칭 노드 또는 다른 네트워크 컴퓨터 장치에서 전형적으로 사용되는 것과 같은 통상적인 또는 주문형 또는 준-주문형 처리기 형태를 할 수 있다. 처리기(22)는 버스(32)로의 출력자료와 버스(32)로의 입력자료에 결합된다.

버스(32)들은 두 개 또는 그이상의 노드들 사이에서 자료를 전송하거나, 그렇지 않으면 이동시킬 수 있다. 가령, 버스(32)들은 공유되는 일반 목적의 버스이거나 특정 노드들 사이에서 특정 타입의 자료를 전송시키도록 될 수도 있다. 버스(32)가 노드들 사이의 경로를 만들도록 하는데 사용하기 위한 인터페이스 회로 및 소프트웨어를 포함할 수 있으며, 상기 노드들을 통해서 자료가 전송될 수 있다. 처리기(22)와 같은 몇가지 장치들은 내부적으로 하나나 둘이상의 버스(32)들을 포함하며 그 속에 있는 내부의 노드들 사이에서 자료를 전송시키도록 한다. 자료로는 처리된 자료, 주소 그리고 제어신호들이 있다.

주메모리(24)는 메개 자료의 저장 및 회수를 제공한다. 가령, 주 메모리(24)는 임의접근 메모리(RAM)이거나 유사회로일 수 있다. 주 메모리(24)는 버스(32)를 통해 처리기(22)와 같은 다른 장치 또는 회로에 의해 접근될 수 있다.

이차 메모리(26)는 자료의 추가저장 및 회를 제공한다. 가령, 부 메모리(26)는 자기 디스크 드라이브, 자기 테이프 드라이브, CD ROMs 과 같은 광학적 판독가능 장치, PCMCIA 카드와 같은 반도체 메모리등과 같은 형태를 한다. 이같은 이차 메모리(26)는 버스(32)를 통하여 처리기(22)와 같은 다른 장치 또는 회로에 의해 접근될 수 있다. 가령, 이차 메모리(26)는 컴퓨터-판독가능 프로그램 코드를 갖는 컴퓨터-사용가능 매체를 포함하는 컴퓨터 프로덕트로 부터 자료를 판독할 수 있다.

I/O 장치(28)는 사용자에게 한 인터페이스를 제공하며, 상기 인터페이스를 통해서 자료가 공유될 수 있다. 가령, 입출력 장치(28)는 키이보드, 태블릿과 스타일러스, 음성 또는 육필 인식기, 또는 또다른 컴퓨터와 같은 잘 알려진 입력장치일 수 있다. I/O 장치(28)는 또한 표시장치 모니터, 플랫 패널 표시장치, 또는 프린터의 형태를 취할 수 있다. I/O 장치(28)는 버스(32)를 경유하여 프로세서(22)와 같은 다른 장치 또는 회로에 의해 접근될 수 있다.

네트워크 통신장치(30)는 다른 컴퓨터 시스템과 같은 다른 계산자원 및 장치로의 인터페이스를 제공한다. 네트워크 통신장치(30)는 자료 통신링크와 네트워크를 통하여 자료통신 스탠다드 및 프로토콜을 실시하기 위한 인터페이스 하드웨어와 소프트웨어를 포함한다. 가령, 네트워크 연결로, 처리기(22)가 한 네트워크를 통하여 자료(가령 정보)를 송신하고 수신할 수 있다. 상기 설명된 장치 및 처리는 컴퓨터 하드웨어와 소프트웨어 기술에 숙련된 자에게 잘 알려진 기술이다.

도 3a 는 본 발명의 실시예에 따라 기록 자료구조(300)의 실시예를 도시한다. 자료구조(300)는 하나의 기호파일(302)과 여러개의 자료파일(304-314)을 포함한다. 파일(304-314)은 가령, 자바(Java™) 클래스 파일, 영상 파일, 오디오 파일, 텍스트 파일 그리고 더욱 추가된 기호파일과 같은 어떠한 디지탈 비트 스트림일 수 있다.

도 3b는 기호파일(302)의 한 실시예를 도시한다. 어떤 실시예에서는, 기호파일이 한 헤더 파일이다. 도시된 실시예에서, 기호파일(302)은 자료파일(304- 314) 각각에 대한 적어도 하나의 식별자(316)를 포함한다. 선택에 따라, 기호파일(302)은 자료파일(304-314) 각각에 대한 추가의 자료(318)를 포함할 수 있다. 가령, 추가의 자료(318)는 파일의 이름, 파일의 작가, 파일의 날짜, 파일의 버전, 파일의 등급(가령 PG와 같은 영화 등급),또는 사용자가 기호파일(302)내에 포함하고자 하는 다른 전자 자료를 더욱더 포함할 수 있다.

기호파일(302)은 한 식별자 ID(320)와 디지탈 기호(322)를 더욱더 포함할 수 있다. 식별자 ID(320)는 기호파일(302)내에 목록된 식별자는 발생시키도록 사용된 알고리즘을 결정하기 위해 필요한 정보를 제공한다. 디지탈 기호(322)는 상기 기호 파일에 대하여 발생된 디지탈 기호를 나타낸다. 상기 디지탈 기호(322), 구조는 물론 이를 발생시키기 위해 사용된 기호 알고리즘에 달려있다.

도 4 는 본 발명의 한 실시예에 따라, 하나 또는 둘이상의 자료파일을 발생시키기 위한 단계(402)를 포함하는 방법(400)을 도시한 도면이다. 가령, 단계(402)는 한 텍스트 파일을 발생시키기 위한 한 텍스트 프로그램, 오디오 또는 비디오 파일을 발생시키기 위한 한 기록 프로그램, 영상 또는 영화파일을 발생시키기 위한 한 그래픽 프로그램, 클래스 파일 또는 프로그램 파일을 발생시키기 위한 프로그래밍 언어 또는 한 자료 파일을 발생시킬 수 있는 어떤 다른 메카니즘을 사용함을 포함한다.

단계(402)에서 하나 혹은 둘이상의 자료파일들을 발생시키었기 때문에, 단계(404)는 이들 자료파일 각각에 대한 식별자를 발생시킴을 포함한다. 단계(404)에서 발생된 식별자들은 가령 한방향 해쉬 기능 알고리즘에 의해 발생되거나, 선택에 따라 주기적 중복 검사합계(CRC)등과 같은 형태를 하기도 한다. 그러나, 한방향 해쉬 기능 알고리즘은 이같은 기능들이 용이하게 발휘될 수 없기 때문에 더욱 완벽한 보안을 제공하게 된다. 일례로서, MD5 및 SHA 와 같은 단일 방향 해쉬 기능 알고리즘은 암호적으로 안전한 것으로 간주된다. 이같은 알고리즘은 컴퓨터 과학 기술에 숙련된자에게 알려져 있다.

다음 단계(406)는 단계(404)에서 발생되는 식별자들을 컴파일하는 한 기호파일을 발생시킴을 포함한다. 가령, 한 기호파일은 식별자를 목록하는 한 텍스트 파일일 수 있다. 선택적으로 한 기호파일은 가령, 각 파일의 이름, 각 파일의 작가, 파일 버전, 파일의 날짜-스탬프 또는 각 자료파일에 관련된 다른 자료를 더욱더 포함할 수 있다. 단계(406)는 자료파일들로 부터 그같은 자료를 문의하고, 트레이스하며, 선택하

고, 그렇지 않으면 모으는 하나 또는 둘이상의 프로그램을 더욱더 포함한다. 단계(406)는 적절한 식별자와 어떤 추가의 자료를 모으기 위해 배치 모드 처리로 자료파일들을 처리하므로써 수행될 수 있다. 당해분야에 숙련된 자라면 방법(400)에 단계에서 단계들을 수행시키는 몇가지 방법으로 기호파일내 목록된 자료를 특별히 오더라고, 그룹으로 하거나 배치시키는데 유익하리라는 것을 이해할 것이다. 가령 상기 식별자와 함께 파일이름 또는 작가를 그룹으로 하는 것이 유용할 수 있다.

일단 기호파일이 발생되기만하면, 단계(408)가 한 기호 알고리즘으로 기호파일을 디지탈 식으로 신호함을 포함한다. 적절한 기호 알고리즘의 예로는 메시지 다이제스트 알고리즘과 RSA 암호화 알고리즘(가령, MD5와 RSA 또는 MD2 와 RSA등)결합 또는 DSA 알고리즘(상기에서 설명됨)을 포함한다. 단계(408)는 공공 또는 개인 키이(Schneier 의 공보참조)에 의해 한 기호 알고리즘으로 기호 파일에 대한 디지탈 기호를 발생시킴을 포함한다.

단계(408)로 부터의 기호파일은 단계(410)에서 수신 사용자에게 제공된다. 단계(410)는 가령 자료버스, 자료링크, 인터넷 또는 몇 개의 다른 컴퓨터 또는 자료통신 네트워크 또는 링크를 통해 사인된 기호파일을 전송시킴을 포함한다. 또한, 단계(410)는 가령 자기저항 매체와 광학적 저장 매체와 같은 컴퓨터 판독가능 매체내에 기호파일을 저장하고, 그리고 컴퓨터 판독가능 매체를 통하여 사인된 기호파일을 한 컴퓨터로 부터 또다른 컴퓨터로 이동시킴을 포함한다.

수신 또는 접근이 있게되자마자, 단계(412)내 수신사용자는 단계(410)내에서 이용될 수 있는 사인된 기호파일의 진짜임을 검증한다. 단계(412)는 가령 키이에 의해 한 기호 알고리즘으로 사인된 기호파일에서의 디지탈 기호를 검증함을 포함한다.

단계(414)는 단계(412)에서 결정된 바와같은 디지탈 기호의 유효함이 방법(400)을 종료시키거나 계속시키는 결정을 나타낸다. 간략하거나 그렇지 않으면 선택을 차지하는 방법(400)으로 도시된때 단계(414)는 단계(412)에서의 사인된 기호파일의 검증이 실패하였음을 기록 또는 표시하거나 그렇지 않으면, 어드레스하는 경보 또는 통지처리, 혹은 로그(log) 처리와 같은 또다른 처리를 호소함을 포함한다.

만약 단계(414)에서의 결정이 파일이 유효하다(즉, 진짜임)는 것이며, 상기 처리가 계속해서 단계(416)로 가며, 이 단계는 기호 파일로 부터 적어도 식별자등을 포함한다. 본 발명의 한 실시예에서, 식별자는 한 안전위치내에 저장된다. 가령 이같은 메모리는 처리가 완성된때 용이하게 클리어되기 때문에, 한 안전위치는 수신 컴퓨터 시스템의 RAM 일 수 있다. 선택에 따라서는 식별자가 한 디스크 또는 테이프 드라이브로 저장될 수 있으며, 이들은 나중의 단계에서 회수될 수 있다. 당해분야에 숙련된 자들이라면 여러가지 자료 저장장치 및 다른 컴퓨터 시스템 구성이 가지각색의 그리고 잠정적인 안전위험(가령, 어떤 저장장치는 다른 저장장치보다 더욱 안전할 것이다)을 내포함을 이해할 것이다. 암호화 및 파일접근 특권과 같은 추가의 안전 대책이 단계 414에서 저장된 바의 기호파일의 신뢰를 더욱더 증가시키도록 사용될 수 있다.

일단 식별자가 단계(416)내에 안전위치에 저장되기만 하면, 식별자가 단계(406)에서 기호파일내에 목록된 자료파일(들)이 단계(418)에서 표시된 바와같은 루우프에 따라 처리될 수 있다.

단계(418)는 가령 단계(420)가 기호파일에 목록된 식별자 수를 기초로하여 임력하여지게될 회수를 반복해서 제어한다. 가령, 기호파일내에 n개의 식별자가 목록되어 있으면(즉, n개의 자료파일이 적재될 것이라면), 한 반복적인 루우프가 i=1 로 부터 i=1 까지 계수하거나, 그렇지 않으면 자료파일 모두가 언제 적재되는지, 혹은 하기에서 설명되는 바와같이 방법(400)에서 나머지 단계에 따라 언제 그같은 적재가 시도되었는가를 결정한다.

단계(420)는 i번째 자료파일을 적재함을 포함한다. 단계(420)는 가령 단계(410)내의 어떠한 방법도 포함하며 한 위치에서 또다른 위치로 i번째 자료파일을 다운로드, 업로드, 방송, 그렇지 않으면 한 위치에서 또다른 위치로 이동시킨다. 일단 i번째 자료파일에 대한 식별기를 제공하고, 계산하며, 또는 발생시킴을 포함한다.

다음에, 단계(424)는 단계(422)에서 제공된 식별기를 단계(416)에서 저장되었던 기호파일내 i번째 자료파일에 대하여 목록된 식별기와 비교함을 포함한다. 만약 식별기들이 부합하면 i번째 자료파일은 진짜인 것으로 검증된다. 만약 식별기들이 부합하지 않으면 i번째 자료파일은 검증된 것으로 보지 않는다.

단계(426)는 단계(424)에서 결정된 바와같은 식별자의 유효함이 단계(418)의 반복적 루우프를 종단시키거나 계속시키는 결정을 제공한다. 만약 i번째 자료파일에 대한 식별자가 단계(424)에서 검증되었으면, 다음에 단계(426)가 i번째 자료파일이 진짜인 것으로 검증되었음을 표시하거나, 기록하거나 혹은 어떤 방법으로든 설정함을 포함하는 단계(428)로 진행시키므로써 단계(418)의 반복적 루우프를 계속한다. 가령 단계(428)는 소스 사용자에 의해 사인된 것으로 i번째 자료파일을 수정 또는 표시함을 포함한다.

반면에, i번째 자료파일에 대한 식별자가 단계(424)에서 진짜인 것으로 검증되지 않는다면, 단계(426)는 단계(430)로 진행하므로써 단계(418)의 반복적 루우프를 종단시킨다. 단계(430)는 어떤 방법으로든 단계(418)의 반복적 루우프를 막아서 단계(428)를 피하고 단계(418)로 되돌아 가도록 한다.

가령 단계(430)는 i번째 자료파일을 무시함을 포함한다. 단계(430)에 추가하여, 다른 단계가 방법(400)내에 포함되어 i번째 자료 파일이 진짜가 아님을 기록하고 혹은 이를 식별하도록 한다.

따라서, 상기의 자료 구조와 단계로, 여러 자료 파일들은 전송하는 사용자는 자료파일 각각에 대하여 분리된 디지탈 기호를 발생시킬 필요없이 기호파일을 발생시키기만 하면되며 그같은 파일을 디지탈 식으로 신호로 표시하기만 하면되므로 관련된 처리시간을 줄이게된다. 마찬가지로, 자료구조와 상기의 단계로 여러자료 파일들을 수신하는 사용자는 관련된 디지탈 기호를 해독하므로써 각 자료파일의 진짜인 것으로 검증하지 않고 그같은 기호파일이 진짜인 것임을 검증하기만하면 되므로 여러자료파일들을 수신하는 사용자는 관련된 처리시간을 줄이게된다. 이같은 하이브리드 검증처리가 기호 및 검증 처리를 합리화한다. 결과적으로 자료파일은 디지탈 식으로 기호로 표시되고, 나중에 적은 시간으로 진짜임이 밝혀진다.

추가로 단계(430)는 시도된 적재를 중지하는 선택적 단계(432)로 그리고 단계(424)에서 진짜임을 검증하

는데 실패함을 경고하는 선택적 단계(434)로 진행된다. 일단 단계(430), 그리고 선택적으로(432) 또는 (434)가 완료되면, 방법(400)이 단계(418)로 되돌아가서 반복적 루우프를 완성하도록 한다. 단계(418)의 반복적 루우프가 완료되면, 방법(400)은 종료된다.

본 발명의 한 실시예에서, 가입자 권한 각각에 대하여 증명서가 발생되며, 즉 한 기호파일에서 독특한 식별자가 증명서로서 구체화된다. 일반적으로, 증명서들은 대개 소스 사용자 컴퓨터 시스템 또는 수신 사용자 컴퓨터 시스템 어느 하나의 한 장소가 자신을 나타내기 위해 사용할 수 있는 토큰(표시)이다. 여러개의 장소들이 단일 증명서와 관련될 수 있다. 선택에 따라서는 여러 증명서가 한 장소와 관련될 수 있다.

소스 사용자 컴퓨터 시스템 및 수신 사용자 컴퓨터 시스템은 자료 파일뿐 아니라 컴퓨터 소프트웨어도 캘리포니아 소재의 Sun Microsystems of Monntain View로 부터 입수될 수 있는 자바 프로그램 언어로 기재된 애플릿의 형태로 교환하도록 구성될 수 있다. 본원 명세서 사용된 바의 애플릿은 대개 서버(server)라고 하는 소스 컴퓨터로부터 고객 컴퓨터 또는 기계로 보내져서, 이미 고객에게 설치된 가령 브라우저 소프트웨어와 같은 소프트웨어와 협력하여 가동되는 소프트웨어 프로그램이다. 설명된 실시예에서, 애플릿은 소스 컴퓨터 혹은 서버로 부터 고객에게로 다운로드된 도 3a 에 관련하여 상기에서 설명된 바의 기록보관 자료 구조로 함께 그룹된 클레스 파일로 부터 얻어진다. 대개, 애플릿은 브라우저 소프트웨어 자신이 수행하도록 되지 않은 다양한 컴퓨터 작업을 수행함으로써 브라우저 소프트웨어로 추가의 기능능력을 제공한다. 따라서, 애플릿을 다운로드한 사용자는 브라우저 소프트웨어에 그렇지 않았으면 브라우저 소프트웨어에 이용될 수 없었던 추가의 기능능력을 제공한다. 이같은 추가의 능력으로는 가령 데이터 베이스로의 고객 인터페이스를 포함할 수 있다.

브라우저와 관련된 안전 관리자는 소스 컴퓨터 또는 고객기계에서 가령 자바 애플릿과 같은 일정 애플릿으로 접근할 수 있는 동작을 제어하도록 사용될 수 있다. 다시말해서, 안전 관리자는 애플릿이 수행하도록 허용된 작용을 제어하고, 그렇지 않으면 애플릿으로의 권한을 연장하도록 사용될 수 있다. 비록 애플릿이 수행하도록 허용되는 작용이 다양하게 변경될 수 있다 하여도 그 작용들은 전부 및 기록작용들이다. 안전 관리자내에서, 각기다른 안전수준이 애플릿에 관련된 각기다른 증명서와 장소에 대한 허용을 정하도록 사용자에게 융통성을 제공하도록 설시될 수 있다. 일반적으로, 사용자는 한 특정 증명서 또는 장소 또는 한 그룹의 증명서 및 장소를 선택하고 그의 선택에 대한 안전 수준을 정할 수 있다.

안전 수준을 실시하기 위해 보안 관리자를 사용하므로써 안전하지 않은 것으로 생각되는 애플릿 작용뿐 아니라 안전한 것으로 생각되는 애플릿 작용을 식별시킴을 필요하게 된다. 하나의 안전작용은 시스템 안전을 위협에 빠뜨리는 또는 고객 또는 서버에게 저장된 정보를 오염시킬 우려가 있는 것으로 생각되지 않는다. 일례로서, 안전작용은 판독 적용작용 또는 특정 리렉토리에 대한 판독 적용작용일 수 있다. 한편, 안전하지 않은 작용은 시스템 안전을 위협하거나 고객 또는 서버에 저장된 정보에 손상을 줄 염려가 있는 어떠한 작용일 수 있다. 안전하지 않은 작용으로는 민감한 서류들로의 접근을 요구하는 기록작용, 삭제작용, 리네임 작용, 그리고 판독작용을 포함할 수 있다. 안전하지 않은 작용은 보호된 원격한 장소로의 연결을 설정하기 위한 요구를 포함한다.

본 발명의 한 실시예에서, 가령 Hot Java™ 브라우저(캘리포니아 소재의 Sun Microsystems of Monntain View으로 부터 입수가능한)와 같은 Java™ 애플릿을 실행할 수 있는 브라우저는 높은 안전수준, 그리고 안전하지 않은 수준을 포함하는 안전 수준의 안전 관리자를 갖는다. 높은 안전수준은 기본적으로 어떠한 안전하지 않은 작용도 차단하면서 한 세트의 안전작용으로 애플릿이 실행될 수 있도록 한다. 설명된 실시예에서, 높은 안전수준은 애플릿이 안전하지 않은 것으로 생각되는 어떠한 작용의 접근도 부정하면서 안전한 것으로 생각되는 대부분의 작용을 가능하게 한다.

한 중간 안전수준은 사용자에게 잠정적으로 안전하지 않을 수 있는 작용을 허용하는 능력을 사용자에게 제공하면서 안전 제한과 함께 애플릿이 실행될 수 있도록 사용될 수 있다. 한 중간안전 수준에서 사용자는 허용가능한 안전한 작용이 아닌 작용의 사용자 인터페이스를 통해서 경고될 수 있다.

설명된 실시예에서, 활동을 설명하는 다이얼로그 박스가 출현하며, 사용자는 잠정적으로 안전하지 않은 작용이 수행될 것을 허락하거나 부정하도록 재촉받게 된다. 낮은 안전수준은 애플릿이 최소의 제한으로 실행되도록 허락하며, 설명된 실시예에서, 잠정적으로 안전하지 않은 작용에 대하여 사용자에게 경고한다. 믿을 수 없는 안전수준은 안전하지 않은 것으로 알려진 증명서와 장소를 나타내도록 사용된다.

도 5 와 관련하여서는 한 안전 관리자에서 안전수준을 정함과 관련된 단계가 본 발명의 한 실시예에 따라 설명될 것이다. 한 실시예에서, 신뢰(트러스트) 및 검증 정함의 수준으로서 알려지기도한 안전수준은 높은 안전수준, 중간 안전수준, 낮은 안전수준 신뢰되지 않은 안전수준등이다. 비록 안전수준이 적절한 그래프 사용자 인터페이스(GUI)의 사용을 통해서 사용자에 의해 정해질 수 있다하여도, 어떠한 적절한 방법도 안전수준을 정하도록 사용될 수 있는 것임을 이해하여야 한다.

안전관리자(500)에서 안전수준을 정하는 처리는 시작되며, 단계(502)에서, 증명서 권한에 대한 안전수준이 정해진다. 증명서 권한은 개별증명서와 증명서 그룹모두에서 각기 다른 안전수준, 또는 우선순위가 적용되도록 한다. 일반적으로 증명서 권한은 특정 증명서가 어떻게 사용될것임을 식별하는 정보를 포함한다. 일례로서, 증명서 권한은 한 증명서가 다른 증명서들을 보증(vouch)할 수 있도록 정해질 수 있다.

증명서 권한에 대한 안전수준이 정해진뒤에, 장소 증명서에 대한 안전수준이 단계(504)에서 정해진다. 장소증명서는 안전 연결을 시작하여 이를통해 트럼잭션이 일어날 수 있도록 정해진 한 장소가 사용할 수 있는 증명서들이다. 장소 증명서에 대한 안전수준은 안전 소켓 층(SSL) 스탠다드 프로토콜 및 안전허용을 명시함을 포함하며, 이를 스탠다드 프로토콜 및 안전허용이 안전 트랜잭션이 연결을 통해 일어나게 되는 그와같은 연결이 진짜임을 증명하도록 사용될 수 있다. 이와같은 안전통신 기술은 잠정적으로 안전하지 못한 장소를 명시하도록 따라서, 더욱 안전한 채널을 제공하여 이용함해 그와같은 장소와의 통신을 피하여 전송이 일어나도록 사용될 수 있다.

단계(506)에서, 소프트웨어 공표자에 대한 안전수준이 정해진다. 인트러네트 환경에서는 그와같은 환경

이 대개 안전한 환경인 것으로 간주되기 때문에 소프트웨어가 증명서와 함께 공표되지 않는다. 따라서, 이와같은 안전환경내에서 공표된 소프트웨어는 안전한 것으로 간주된다. 그러나, 가령 인터넷 환경에서처럼 소프트웨어가 증명서와 함께 공표되는 환경의 경우, 증명서는 증명서들과 관련된 소프트웨어 코드가 브라우저 실행을 위해 신뢰되는 가에 대하여 결정하도록 사용될 수 있다.

장소 이름들에 대한 안전수준이 단계(608)에서 정해진다. 장소 이름들에 대한 안전수준을 정하는 과정은 한 안전수준이 한 장소에 대하여 정해진때 그와같은 안전수준이 상기 장소와 관련된 모든 소프트웨어로 적용됨을 제외하고는 소프트웨어 공표자들을 정하기 위한 처리와 기본적으로 동일하다. 장소이름 허락을 정하므로써 증명서 없는 소프트웨어가 시스템 자원을 간섭하게되는 위험없이 검사될 수 있도록 한다. 다음에, 증명서 타입이 단계(510)에서 정해진다. 증명서 타입을 세트하는 것은 어떻게 증명서가 사용될 것인가를 결정하고, 그 증명서가 어떻게 사용될 것으로 기대되는가에 따라 증명서들에 대한 권한을 선택할 수 있다. 증명서 장소가 단계(510)에서 정해진뒤에, 안전수준을 정하는 처리가 완성된다. 안전순서가 정해지는 순서는 특정 보안 관리자의 요구사항에 따라 광범위하게 변경될 수 있다.

어떤 실시예에서는, 추가의 개선된 세팅이 안전수준을 정하도록 사용될 수 있다. 한 실시예에서, 개선된 세팅은 GUI 또는 유사한 접속장치를 통해서 사용자가 수정할 수 있는 제어이며, 사용자로 하여금 개별 증명서 권한, 장소 증명서, 소프트웨어 공표자 또는 장소 이름들에 대한 특정의 주문 안전수준을 정할 수 있도록 한다. 또한 개선된 세팅은 사용자가 한 그룹의 증명서 권한, 장소 증명서, 소프트웨어 공표자 또는 장소 이름들에 대한 안전수준을 주문에 의해 정할 수 있도록 구성될 수 있다. 따라서, 개선된 세팅은 대체로 안전수준을 제어하고 전체 증명서 처리에 있어서 융통성을 제공한다. 일례로서, 개선된 세팅의 사용을 통해, 사용자는 특정 장소 증명서를 한 중간 보강 수준으로 정할 수 있으며, 또한 상기 장소 증명서와 관련된 안전허용이 판독 접근을 허락하는 것만으로 제한될을 명시하는 바이다. 또한 개선된 세팅은 임의적인 수준으로 내용을 번복하도록 사용될 수 있으며, 가령 개선된 세팅은 어떤 안전수준에서는 대개 허용되지 않는 허락을 허용하도록 사용될 수 있다.

설명된 실시예에서, 개선된 세팅이 제공되어 높은 안전수준, 중간 안전수준, 낮은 안전수준, 그리고 앞서 설명된 신뢰할 수 없는 안전수준 외에도 추가의 선택이 가능하며 사용자가 가령 선택된 안전수준 이외로 실시될 수 있는 한 장소 증명서에 대한 특정허용을 선택하도록 할 수 있다. 이들 특정 허용으로는 사용자에게 경고 메시지를 제공하지 않고 애플릿이 원도우를 개방하도록하며, 경고 다이얼로그없이 또는 경고 다이얼로그와 함께 자동으로 로컬 적용을 알으킬 수 있도록 하고, 경고 다이얼로그 없이 애플릿이 모든 특정에 접근하도록 허용하며, 그리고 경고 다이얼로그 없이 애플릿이 실행을 시작할 수 있도록 함을 포함한다.

도 5a 는 본 발명의 실시예에 따라 개선된 세팅을 설명하는 브라우저 인터페이스를 개략적으로 도시한 도면이다. 앞서 설명한 바와같이, 개선된 세팅은 상기 브라우저 인터페이스가 제공된 안전수준에 추가하여 가능하게 되거나 불가능하게 될 수 있는 특정한 허용을 선택하도록 사용될 수 있다. 비록 브라우저 인터페이스(560)가 어떤 적절한 브라우저 인터페이스(560)일 수도 있으나, 설명된 실시예에서, 브라우저 인터페이스(560)는 HotJava™ 브라우저의 대표적인 것일 수 있다. 도시된 바와같이, 브라우저 인터페이스(560)는 개선된 세팅 표시장치 윈도우(564)를 포함한다. 표시장치 윈도우(564)의 첫 번째 영역(568)은 장소와 증명서(570), 그리고 한 그룹의 장소들과 증명서들을 포함하며, 이들에 대해서는 안전허용이 주문으로 결정될 수 있다. 애플릿 허용(572), 파일접근(574), 그리고 네트워크 접근(576)들은 주문으로 정해질 수 있는 허용들 가운데 하나이다. 설명된 실시예에서, 한 선택(580)은 파일접근(574)에 대한 즉 애플릿이 접근하도록 허용된 파일이 정해질 것임을 나타낸다.

두 번째 서브-영역(582)은 파일들과 디렉토리(584)들을 표시하며, 선택되는 때 선택된 세팅, 즉 애플릿 허용(572) 명령을 사용하여 결정된 세팅을 갖는 애플릿이 이들로 부터 판독할 수 있도록 허용된다. 이와 유사하게, 세 번째 서브-영역(586)은 파일들과 디렉토리(590)들을 표시하며, 이들 파일들과 디렉토리들로 적절한 허용이 인정된 애플릿이 기록하도록 허용된다. 가령 다른 파일들로의 접근을 허용하기전에 경고 선택(594) 또는 애플릿이 한 파일을 삭제하려는때 경고 선택(590)과 같은 추가의 선택가능한 선택을 하므로써 사용자가 안전선택을 주문으로 만들 수 있도록 한다.

도 6 은 본 발명의 한 실시예에 따라 검증세팅을 사용하는 애플릿을 실행하는 한 처리와 관련된 단계들을 설명한다. 검증 세팅을 실시하는 처리는 시작되며, 단계(602)에서 애플릿이 실행되게될 로컬머신으로 한 애플릿이 다운로드된다. 설명된 실시예에서, 애플릿을 다운로딩하므로써 클래스 파일들을 담고있는 기록보관 파일 또는 기록보관 자료구조의 적어도 일부를 다운로딩함을 수반하게 된다. 애플릿이 다운로드된 뒤에 기호가 표시된 기록보관 스트림은 단계(604)에서 수신된다. 설명된 실시예에서, 기록보관 스트림은 Java™(자바) 기록보관 파일과 관련된 한 디지탈 기호를 포함한다.

단계(606)에서, 기호로 표시된 기록보관 스트림내 기호가 유효한가, 즉 기호가 허용가능한가에 대하여 결정이 있게된다. 기호로 표시된 기록보관 스트림이 앞서 설명된 기호로 표시된 신호파일의 한 실시예이다. 기록보관 스트림내의 기호가 유효한가에 대한 결정은 한 공지의 권한이 발견될 때까지 한 기호 파일내 증명서들과 같은 일련의 권한들을 체계적으로 조사함을 포함한다. 다음에 공지의 권한이 유효함에 대하여 조사된다. 일례로서 증명서 A는 유효한 증명서인 것으로 알려져 있는 증명서 B에 의해 보증된다. 따라서, 증명서 B가 유효한 것으로 알려진때 증명서 A는 유효한 것으로 간주될 수 있다.

기호가 유효하다는 결정이 있게되면, 처리흐름이 단계(608)로 전행되며, 이 단계에서 애플릿이 브랜드(brand)된다. 애플릿을 브랜딩하거나 마킹(표시)하는 것은 애플릿에 기호표시기를 부착시키거나, 애플릿이 유효함을 나타내도록 사용될 수 있는 식별자를 애플릿으로 부착시킴을 나타내는 것이다. 일단 애플릿이 적절하게 브랜드되면, 이 애플릿은 단계(610)에서 실행된다. 애플릿이 실행되는 동안, 애플릿내의 다양한 작용이 호출된다.

단계(612)에서는 애플릿이 실행을 종료하였는가에 대한 결정이 이루어진다. 다시말해서, 애플릿과 관련된 각 작용이 하기에서 설명되는 바와같이 실행되었는지 혹은 실행이 허용되지 않았는지 결정된다. 애플릿을 실행하는 처리는 종료된다. 애플릿 실행이 종료되지 않았음이 결정되면, 단계(614)에서는 애플릿

작용이 안전검사를 트리거하는가가 결정된다. 즉, 단계(614)에서, 특정한 애플릿 작용이 사용자의 시스템 안전에 일시적으로 해로운 것으로 결정된 그와같은 작용에 속하는가에 대한 결정이 있게된다. 이와같은 작용은 컴퓨터분야, 특히 컴퓨터보안 기술분야에 숙련자에게는 잘 알려진 것이다. 일례로서, 사용자의 시스템 보안에 일시적으로 해로운 작용들로는 제한되지 않은 기록접근, 시스템 자원의 수정, 그리고 다른 시스템들로의 개방된 전송등이 있다.

애플릿 작용이 보안 검사를 트리거하면, 단계(608)에서 애플릿상에 있는 브런드가 단계(616)에서 사용자에 의해 앞서 제공된 보안 세팅 또는 허용수준과 비교된다. 어떤 실시예에서는 보안 세팅을 애플릿상의 브런드와 비교하는 것이 사용자 인터페이스를 통하여 사용자와 협의함을 포함한다. 이같은 실시예에서는 사용자가 보안 세팅의 바이패스를 허락할 수 있으며, 즉 사용자가 한 특정작용을 허용하거나 부정하기위해 보안 세팅들을 무시할 수 있다. 단계(616)로 부터 애플릿 작용에 대한 보안이 만족스러운가에 대한 결정이 있게되는 단계(618)로 처리제어가 진행된다. 만약 보안이 만족스러우면, 애플릿상에 있는 브런드가 보안 세팅보다 낮다는 사실에 의해 혹은 사용자가 상기 애플릿 작용을 허용함에 의해 애플릿 작용이 단계(620)에서 허용된다. 반면에, 만약 보안이 단계(618)에서 만족되지 않으면, 애플릿 작용은 단계(622)에서 허용되지 않는다. 애플릿 작용이 허용되지 않은뒤에는 처리제어가 애플릿이 계속해서 실행되는 단계(610)로 되돌아간다.

애플릿 작용이 단계(614)에서 한 보안 검사를 조사하지 않으면, 다음에 처리흐름은 단계(610)로 되돌아가며, 상기 단계에서 애플릿이 계속해서 실행된다. 애플릿이 실행을 끝내거나 단계(614)에서 현재의 애플릿 작용이 한 보안 검사를 트리거하는 결정이 있게되어 처리제어가 앞서 설명된 바와같이 단계(618)로 진행되는 때까지 단계(610)와 단계(614) 사이에서 처리흐름이 계속해서 순환된다.

단계(606)에서 기호의 유효함에 대한 조사로 되돌아가서, 만약 기호가 유효하지 않다는 결정이 있게되면, 기록보관은 기호가 표시되지 않을 것으로 간주되며, 처리흐름이 기호가 표시되지 않은 스트림이 허용되어야 하는가에 대한 결정이 있게되는 단계(624)로 진행된다. 설명된 실시예에서, 기호가 표시되지 않는 스트림이 허용되어야 하는가에 대한 결정은 사용자 인터페이스 사용을 통해 사용자에 의해 이루어진다. 일례로서, 사용자는 기호가 유효하지 않은등만 그가 애플릿을 실행하는 결정을 할 수 있음을 나타내는 경고 다이얼로그로 자극을 받을 수 있다. 만약 기호가 표시되지 않은 스트림이 허용될 것이라는 결정이 있게되면, 처리 흐름이 단계(608)로 진행되며, 여기서 애플릿이 적절하게 브런드된다. 즉 애플릿에 관련된 스트림이 기호가 표시되지 않은 스트림이 허용되지 않는 것이며, 애플릿이 정지되거나 단계(626)에서 실행되지 않도록 할 것이라면, 애플릿을 실행시키는 처리는 종료된다.

도 7 에서는 컴퓨터 네트워크에서의 연결을 설정시킴과 관련된 단계가 본 발명의 한 실시예에 따라 경정된 것이다. 이같이 연결시키는 처리(700)는 단계(702)에서 시작되며, 여기서 필요한 연결이 만들어진다. 설명된 실시예에서, 필요한 연결을 만드는 것은 연결이 필요로되는 장소에 대한 유니버설 기존언어(URC) 주소를 명시함을 포함한다. 연결이 만들어진후, 단계(704)에서 연결이 있고자하는 장소에서 통신이 설정된다.

단계(704)로 부터 처리 제어가 단계(705)로 진행되며 장소가 보안 연결을 필요로 하는 가에 대한 결정이 있게된다. 한 실시예에서, 한 보안 연결은 본 발명 기술분야에서 숙련된 자에 의해 이해되어지는 바의 한 보안 소켓층(SSL)을 통한 연결이다. 한 보안연결이 필요하지 않은 것으로 결정되면, 그와같은 장소로의 연결이 단계(708)에서 있게되며, 한 연결을 설정하는 처리가 완성된다.

만약 상기 장소가 한 보안연결을 필요로하는 결정이 있게되면, 다음에 단계(710)에서는 그 장소와 관련된 장소 증명서가 유효한가가 결정한다. 한 장소 증명서는 신뢰되지 않은 한 장소 또는 안전하지 않은 것으로 암려진 한 장소에 대한 유효한 증명서일 수 있기 때문에 유효한 장소 증명서가 신뢰된 장소 증명서임을 필요는 없다. 만약 장소 증명서가 유효하면, 처리흐름이 단계(712)로 진행되며, 이 단계에서 장소 증명서가 신뢰되는 가에 대한 결정이 있게된다. 장소 증명서가 신뢰되는 결정이 있게되면, 처리흐름이 단계(708)로 진행되며, 여기서 상기 장소로의 연결이 있게된다. 선택에 따라, 장소 증명서가 신뢰되지 않는다는 결정이 있게되면, 단계(714)에서 이 장소(단계 704)와 설정된 통신이 종료된다. 이와유사하게, 장소 증명서가 유효하지 않다는 것이 단계(710)에서 결정되면, 그와같은 장소와의 통신이 단계(714)에서 종료된다.

상기에서 설명된 바의 본 발명의 실시예는 컴퓨터 시스템내에 저장된 자료를 포함하는 다양한 처리단계를 사용한다. 이들 단계들은 물리량에 대한 물리적 조작을 필요로 한다. 대개, 이들 물리량들은 저장되고, 전달되며, 비교되고, 그리고 조작될 수 있는 전기적 또는 기계적 신호 형태를 갖는다. 상기 신호들을 비트, 값, 엘리먼트, 변수, 문자, 자료구조 등으로 언급하는 것이 때때로 편리한때, 이는 이같은 용어들이 일반적으로 이용되기 때문이다. 그러나 이들 모두 및 유사한 용어는 적절한 물리량과 관련되어야 하며 이들 물리량들로 적용된 편리한 표시에 불과한 것이다.

또한, 수행된 조작들은 발생시키고, 계산하며, 표시(마킹)하며, 무시하고, 삭제하며, 경고하고, 검증하며, 신호로 표시하고, 전송하며, 수신하고 발생시키며, 반복하고, 식별하며, 실행하고, 혹은 비교하는 등의 용어를 말하는 것이다. 본 발명의 실시예 일부를 형성하는 본원 명세서에서 설명된 어느 동작에서도, 상기 동작은 기계 동작을 말하는 것이다. 본 발명의 실시예 동작을 수행하기 위한 유용한 기계는 범용 디지탈 컴퓨터 또는 다른 유사장치를 포함한다. 모든 경우에서, 컴퓨터를 동작시키는 동작 방법과 컴퓨테이션 자체의 방법에는 차이가 있다는 것을 이해하여야 한다. 본 발명의 한 실시예는 필요한 물리적 신호를 발생시키기 위해 전기적 또는 다른 물리적 신호를 처리하는데 컴퓨터를 동작시키기 위한 방법 단계들에 대한 것이다.

본 발명의 요약

본 발명의 실시예는 이들 동작을 수행하기 위한 장치에 대한 것이기도하다. 이같은 장치는 필요한 목적으로 특별히 구성될 수 있으며, 혹은 컴퓨터내에 저장된 컴퓨터 프로그램에 의해 선택적으로 작동되거나 재구성된 범용 컴퓨터일 수 있다.

본원 명세서에서 제시된 처리는 고유하게 어떤 특정 컴퓨터에 대한 것은 아니다. 특히, 범용 머신이 본원 발명의 가르침에 따라 기록된 프로그램과 함께 사용될 수 있으며, 혹은 필요한 방법단계들을 수행하기 위해 더욱 특수한 장치를 구성하기 위해 더욱 편리해질 수 있다. 다양한 머신들에 대한 필요한 구조는 상기 설명으로 부터 실시될 수 있다.

또한 본 발명의 실시예는 다양한 컴퓨터 실시동작을 수행하기 위한 프로그램 지시들을 포함하는 컴퓨터 판독가능 매체에 대한 것이다. 매체(media) 및 프로그램 지시들은 본 발명의 실시 목적을 위해 특별히 디자인되고 구성되며, 혹은 이들은 컴퓨터 소프트웨어 기술분야에서 잘 알려진 것들이다. 컴퓨터-판독가능 매체의 예로서는 하드 디스크, 플로피 디스크, 자기 테이프와 같은 자기매체, CD-ROM 디스크와 같은 광학적 매체, 플롭티클 디스크와 같은 자기-광학 매체, 판독전용 기억장치(ROM), 임의 접근 기억장치(RAM)와 같은 프로그램 지시들을 저장하고 수행하도록 된 하드웨어 장치등이 있다.

프로그램 지시의 예로는 컴파일러에 의해 발생되는 머신 코드, 인터프리터를 사용하여 컴퓨터에 의해 실행될 수 있는 고수준 코드를 포함하는 파일을 모두 포함한다.

본 발명은 발명의 사상을 벗어나지 않는 한도에서 수정 또는 변경될 수 있다. 가령, 식별자 또는 기호 알고리즘이 더욱더 선택되거나 수정되고 익스포트 조절에 적합하도록 사용이 제한될 수도 있다. 이는 자료파일의 금로별 교환을 제공하는 컴퓨터 네트워크인 경우에 더욱 적용된다.

검증 세팅을 사용하는 애플릿을 실행함과 관련된 단계들, 한 장소로의 연결을 설정함과 관련된 단계등이 다시 배열될 수 있다. 이같은 단계들이 본 발명의 사상을 벗어나지 않는 한도에서 추가되기도, 혹은 삭제되기도 한다.

또한 몇 개의 보안 수준만이 명시되었으나 특정 컴퓨터 시스템의 요구조건에 따라 이같은 보안 수준이 광범위하게 변경될 수 있다.

(57) 청구의 범위

청구항 1. 적어도 하나의 자료파일과 기호파일을 수신하고, 이때 자료파일과 기호파일이 분리되어 있고, 상기 자료파일이 한 식별자를 포함하며, 기호파일은 자료파일을 위한 식별자와 디지탈 기호를 포함하고, 그리고

기호파일이 진짜임을 결정하기 위해 컴퓨터 시스템을 사용하여 기호파일을 처리함을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 2. 제 1 항에 있어서, 자료파일이 진짜임을 결정하기 위해 컴퓨터 시스템을 사용하여 자료파일내의 식별자와 기호파일내의 식별자를 비교하며, 기호파일을 처리함이 기호파일이 진짜임을 결정하기 위해 컴퓨터 시스템을 사용하여 디지탈 기호를 처리함을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 3. 제 2 항에 있어서, 자료와 기초 파일내의 식별자가 부합하는때 기호로 표시된 바와같이 자료파일을 표시함을 더욱더 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 4. 제 2 항 또는 3 항에 있어서, 자료와 기호파일내 식별자들이 부합하지 않는때, 자료파일을 무시하고, 자료파일의 복제를 삭제하며, 그리고 사용자를 경고하는 그룹으로 부터 선택된 적어도 하나의 조작을 더욱더 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 5. 제 2 항 내지 4 항중 어느 한항에 있어서, 컴퓨터 시스템을 사용하여 자료파일내의 식별자를 기호 파일내의 식별자와 비교함이 두 번째 자료파일에 대하여 반복되는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 6. 전술한 항중 어느 한항에 있어서, 디지탈 기호를 처리함이 한 기호 알고리즘으로 디지탈 기호를 검증함을 더욱더 포함하고, 기호 알고리즘이 한 키이(key)된 알고리즘이며, 상기 기호 알고리즘이 DSA 알고리즘, 그리고 메시지 다이제스트와 RSA 결합 알고리즘의 그룹으로 부터 선택되는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 7. 전술한 항중 어느 한항에 있어서, 식별기가 단일방향 해쉬 기능 알고리즘과 주기적 반복검사 합계 알고리즘중 한 알고리즘을 사용하여 발생되는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 8. 전술한 항중 어느 한항에 있어서, 자료파일내 식별자를 기호 파일내 식별자와 비교하는 것이 단일 방향 해쉬 기능 알고리즘으로 식별자 하나 또는 둘이상을 발생시킴을 더욱더 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 9. 전술한 항중 어느 한항에 있어서, 자료파일내 식별자를 기호파일내 식별자와 비교하는 것이 주기적 중복 검사합계 알고리즘으로 식별자 하나 또는 둘이상을 검사함을 더욱더 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 10. 전술한 항중 한항에 있어서, 자료파일과 기호파일이 네트워크 컴퓨터들 가운데에서 자료파일과 기호파일을 전달시킴을 더욱더 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 11. 전술한 항중 한항에 있어서, 자료파일내 식별자가 증명서 권한, 사이트 증명서, 소프트웨어 공표자 식별자 그리고 사이트(장소)이름중 적어도 하나를 포함하며, 그리고

상기 방법이 상기 증명서 권한, 사이트 증명서, 소프트웨어 공표자 식별자 그리고 사이트 이름중 적어도 하나에 대한 보안 수준을 정함을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 12. 제 11 항에 있어서, 상기 자료파일을 컴퓨터 시스템으로 다운로딩함을 포함하고, 그리고 상기 자료파일이 한 애플릿을 포함하며 디지탈 기호가 검증된때, 상기 방법이 애플릿을 검증된 것으로 브랜

담하고 등 애플릿을 실행시킴을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 19. 제 12 항에 있어서, 자료파일이 한 애플릿을 포함하고, 기호가 검증되지 않은때, 상기 방법이 기호로 표시되지 않는 자료파일이 컴퓨터에서의 실행에 대하여 허용될 수 있는지에 대하여 결정하고, 만약 기호로 표시되지 않은 자료파일이 상기 컴퓨터에서의 실행에 대하여 허용될 수 없다면 상기 애플릿을 종료시킴을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 14. 제 13 항에 있어서, 기호로 표시되지 않은 자료파일이 상기 컴퓨터에서의 실행에 대하여 허용될 수 있는 것으로 결정되는때 애플릿을 브랜딩함을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 15. 제 14 항에 있어서, 애플릿을 실행함을 포함하고 애플릿을 보안검사를 트리거하는 한 작용을 수행하는가를 결정함을 포함하고, 이때 상기 보안검사가 브랜드를 보안 수준과 비교하고 보안검사가 만족되는때 그와같은 작용을 허용하며, 그리고 보안검사가 만족되지 않는때 그와같은 작용을 허용하지 않음을 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 16. 전술한 항중 어느 한항에 있어서, 컴퓨터 시스템을 사용하여 원격한 장소와의 자료통신 연결을 설정하고, 그같은 장소가 보안 연결을 필요로하는가를 결정하며, 상기 장소에 대한 장소 증명서가 보안 연결이 필요로하는 결정에 응답해서 유효한가를 결정함을 더욱더 포함하는 자료가 진짜임을 검증하기 위한 컴퓨터 실시방법.

청구항 17. 자료파일이 한 식별자를 포함하며, 기호파일은 자료파일을 위한 식별자와 디지탈 기호를 포함하는 적어도 하나의 자료파일과 한 기호파일의 진짜임을 검증하기 위한 장치로서,

기호파일이 진짜임을 결정하기 위해 디지탈 기호를 처리하기 위한 처리기, 그리고

자료파일의 진짜임을 결정하기 위해 컴퓨터 시스템을 사용하는 자료파일내의 식별자를 기호파일내의 식별자와 비교하기 위한 비교기를 포함하는 적어도 하나의 자료파일과 한 기호파일의 진짜임을 검증하기 위한 처리기.

청구항 18. 제 17 항에 있어서, 컴퓨터 시스템을 사용하여 자료파일내의 식별자와 기호파일내의 식별자를 비교하기 위한 비교기가 자료와 기호파일내 식별자들이 부합하는때 기호로 표시된 바와같이 자료파일 표시하기 위한 마커(표시기)를 더욱더 포함하는 적어도 하나의 자료파일과 한 기호파일의 진짜임을 검증하기 위한 처리기.

청구항 19. 자료가 진짜임을 검증하는데 사용하기 위해 구체화된 컴퓨터-판독가능 코드를 갖는 컴퓨터-사용가능 매체를 포함하는 컴퓨터 프로그램 프로덕트로서, 컴퓨터 시스템으로

a) 적어도 하나의 자료파일과 기호파일을 수신하며, 자료파일은 식별자를 포함하고, 기호파일은 자료파일과 디지탈 기호를 위한 식별자를 포함하며,

b) 기호파일의 진짜임을 결정하기 위해 컴퓨터 시스템을 사용하여 기호파일을 처리하기 위해 컴퓨터-판독가능 프로그램 코드를 포함하는 컴퓨터 프로그램 프로덕트.

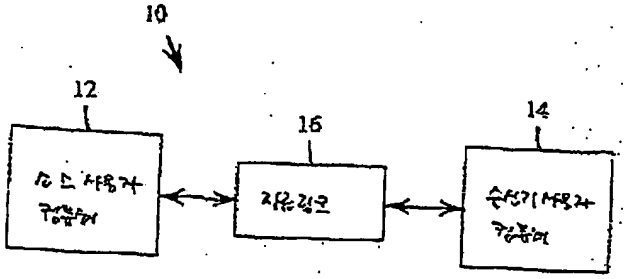
청구항 20. 제 19 항에 있어서, 컴퓨터 시스템을 사용하여 자료파일내 식별자를 기호파일내 식별자와 비교하여 자료파일의 진짜임을 결정하도록 하고, 이때 기호파일을 처리하는 것이 자료파일의 진짜임을 결정하기 위해 컴퓨터 시스템을 사용하여 디지탈 기호를 처리함을 포함하는

컴퓨터-판독가능 프로그램 코드를 더욱더 포함하는 컴퓨터 프로그램 프로덕트.

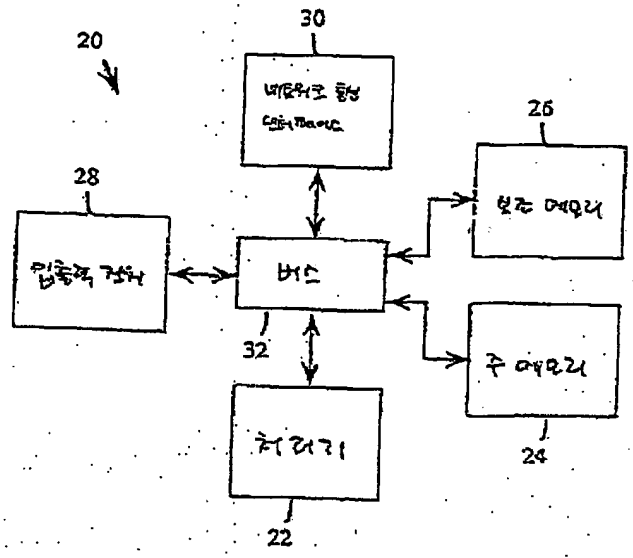
청구항 21. 제 20 항에 있어서, 컴퓨터 시스템을 사용하여 자료파일내 식별자를 기호파일내 식별자와 비교함이 자료와 기호파일내 식별자가 부합하는때 기호로 표시된 바와 같이 자료파일을 표시함을 더욱더 포함하는 컴퓨터-판독가능 프로그램 코드를 더욱더 포함하는 컴퓨터 프로그램 프로덕트.

도면

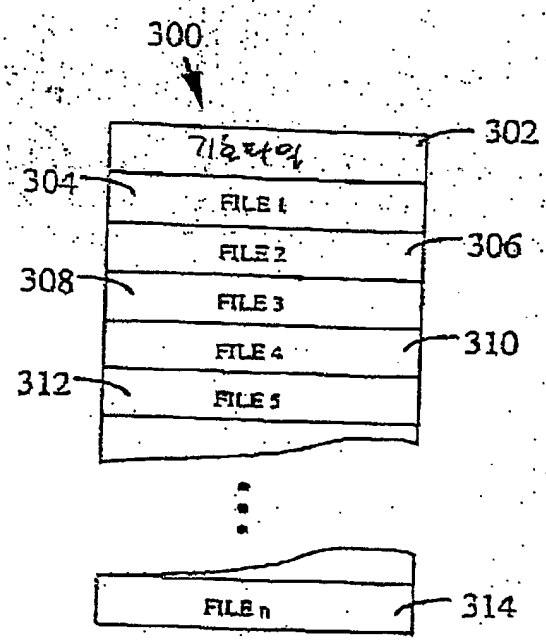
도면1



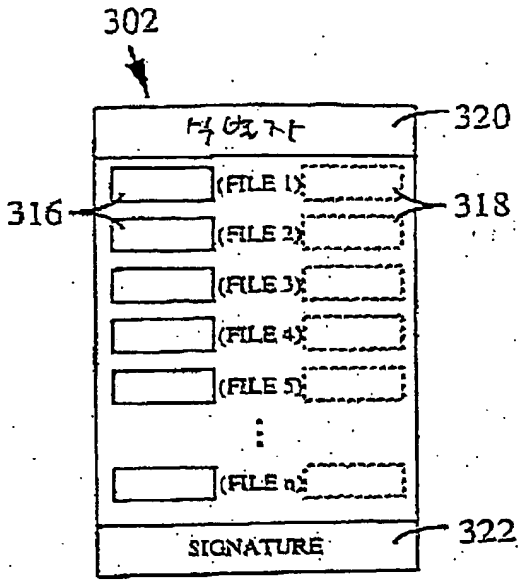
도면2


20
30
28
26
24
32
22
버스
처리기

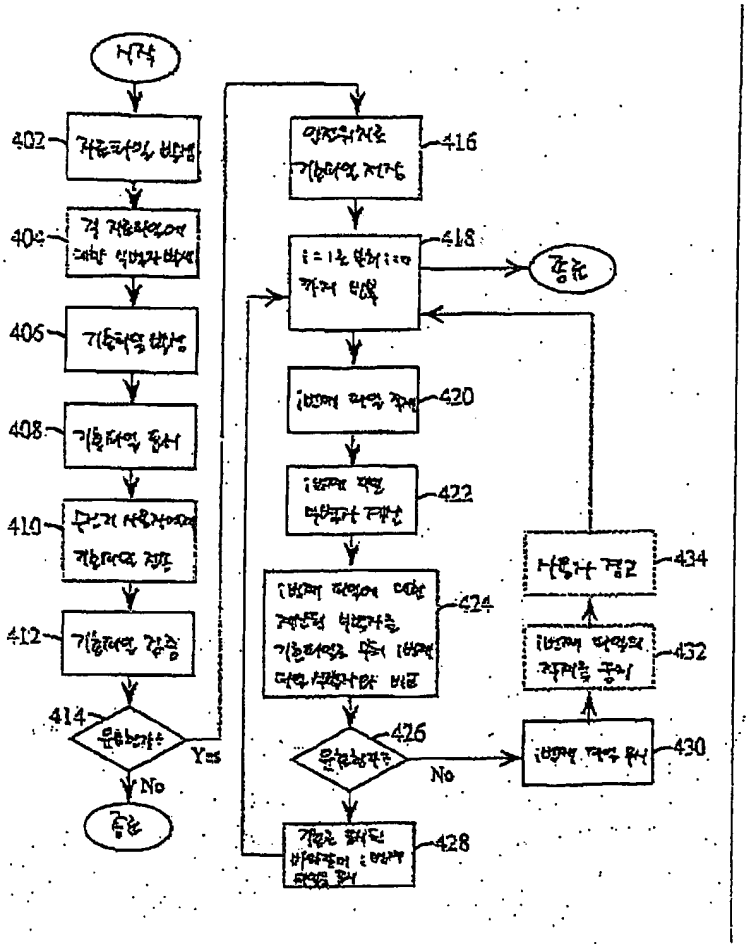
도면3a


300
302
304
306
308
310
312
314
FILE 1
FILE 2
FILE 3
FILE 4
FILE 5
FILE n

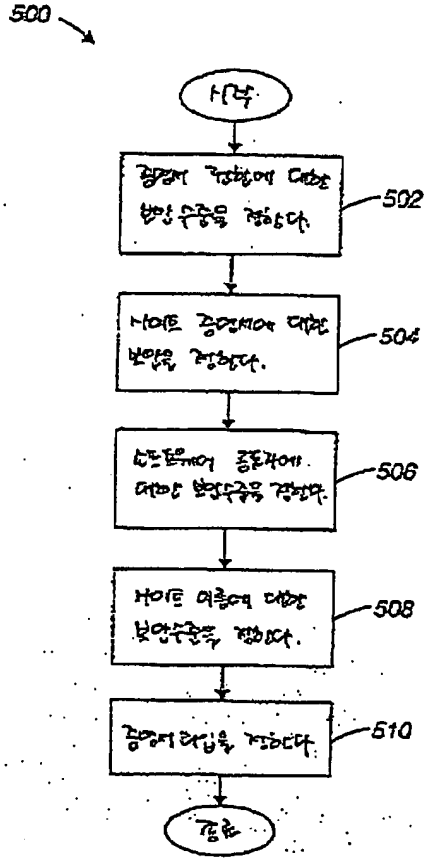
도면3


302
헤더부
320
316
318
(FILE 1)
(FILE 2)
(FILE 3)
(FILE 4)
(FILE 5)
(FILE n)
SIGNATURE
322

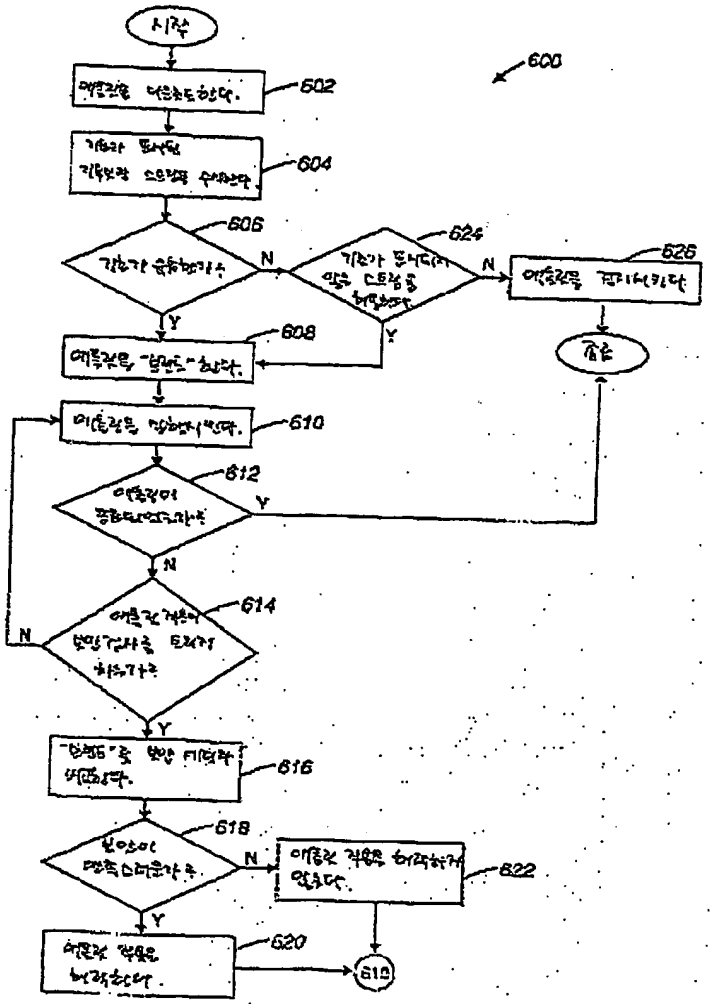
도면4


시작
402
404
406
408
410
412
414
Yes
No
종료
416
418
420
422
424
426
No
428
430
432
434

도05



도면8



도면7